

Serial No. 09/468,377
Art Unit No. 2134

REMARKS

Claims 1-17 are currently pending in the patent application. The Examiner has rejected Claims 1-3, 5-7, 12-13, 15, and 16 under 35 USC 103 as unpatentable over the teachings of Mi in view of Olden and Aziz; Claims 4 and 8 as unpatentable over Mi in view of Olden and Aziz and further in view of Thomlinson; Claims 9-10, 14, and 17 as unpatentable over Mi in view of Olden and Aziz and further in view of Jablon and Thomlinson; and, Claim 11 as being unpatentable over the teachings of Mi in view of Olden, Aziz, and Jablon and further in view of Schneier. For the reasons set forth below, Applicants respectfully assert that all of the pending claims are patentable over the cited prior art.

The present invention is a computer program product and method for securely providing data of a content provider to a user without trusting an internet service provider. As Applicants had previously argued, the present invention allows secure data transfer between a content provider and a user without having the internet service provider participate in the security features, such that transmitted

Y0999-558

-12-

Serial No. 09/468,377

Art Unit No. 2134

data is always encrypted. In that way, a user could access the internet through any service provider, without sharing any security information with the internet service provider. Similarly, the content provider could securely transmit encrypted data to a trusted user, without concern that the internet service provider, or other customers of the internet service provider, could access the content provider's data. The security relationship is between the content provider and the user and the claims expressly recite steps for exchanging encryption keys and passwords only between the user and the content provider. By the previous amendments, Applicants have ensured that all of the claims expressly recite that the content provider is not the internet service provider and that the secure transmission is done without trusting the internet service provider.

The Examiner has newly cited the Mi patent as the primary reference in the Office Action. The Mi patent is directed to a system and method for using an internet-based caller ID to control client access to an object stored on a server. Under the Mi method, upon receipt of a client request, the server generates a DLL file 407 having a secret key 418 (Col. 7, lines 23-26) and sends the DLL file with an

YO999-558

-13-

Serial No. 09/468,377
Art Unit No. 2134

applet to the client browser (Col. 7, lines 27-33 and 41-44). At the client, the DLL file is executed so that the client uses the same secret key 418 from the DLL file, as well as its processor number 422 which is known to the server (Col. 6, lines 56-67) to calculate a hash value which is returned to the server (Col. 8, lines 4-9 and 32-35). When the server receives the hash value from the client, the server's comparison agent calculates a hash value, compares it to the received hash value, and allows the client access to the data if the two values compare favorably (Col. 8, lines 36-44). For each session, the DLL file will contain a different secret key (Col. 7, lines 26-27 and Col. 8, lines 49-53) which is known to both the server and the client.

Applicants respectfully disagree with the Examiner's interpretation of the teachings of the Mi patent. The Examiner has concluded that Mi teaches the steps of generating a first key known only to the content provider, encrypting a second key using the first key, decrypting the second key using the first key when the user desires access to data, and accessing the data using the second key. Applicants respectfully disagree. The Mi patent teaches that secret key 418 is send from the server to the client

YO999-558

-14-

Serial No. 09/468,377
Art Unit No. 2134

and is used by the applet at the client to calculate a second "key", the hash value. Mi does not teach that the secret key is known only to the server and does not teach that a second key is encrypted using the secret key and an encryption algorithm requiring a one-time password. Mi's session-based secret key 418 is known to both the server and the client and is used to calculate a hash value which is transmitted back to the server.

Applicants respectfully assert that the Examiner has not established a *prima facie* case of obviousness, since the Examiner has not provided prior art which teaches or suggests all of the claims limitations (*In re Wilson*, 424 F. 2d 1382, 165 U.S.P.Q. 494 (C.C.P.A. 1970)). The Mi patent does not teach or suggest the claimed means or steps for generating a first key known only to the content provider and encrypting a second key using the first key and an encryption algorithm. The cited teachings from Col. 8, lines 4-10 and from Col. 4, lines 21-28 teach calculating a hash value with the secret key 418 which is known to both the server and the client. Further, the Mi patent does not teach the claimed step of decrypting the second key using the first key. The cited teachings from Col. 8, lines 32-46

YO999-558

-15-

Serial No. 09/468,377
Art Unit No. 2134

teach that the server calculates a hash value using secret key 418 and compares it to the received hash value which was calculated at the client using secret key 418. The cited passage does not teach that the client-generated hash value is decrypted using secret key 418. Clearly, therefore, the Mi patent does not provide teachings or suggestions of the claim limitations.

The Examiner has additionally cited the Aziz patent for its teachings regarding a one-time password and the Olden patent for teaching storing on an encrypted second key on a client machine. Applicants respectfully assert, however, that neither Aziz nor Olden teaches or suggests the claimed means or steps for generating a first key known only to the content provider, encrypting a second key using the first key, or of decrypting the second key using the first key. Absent some teachings or suggestions of those claimed features, a holding of obviousness simply cannot be maintained. Since all of independent Claims 1, 5, 12, 13, 15 and 16 include the foregoing claim features, as do the claims which depend therefrom, Applicants conclude that a *prima facie* case of obviousness has not been established and

YO999-558

-16-

Serial No. 09/468,377
Art Unit No. 2134

respectfully request withdrawal of the rejections based on the combination of Mi, Aziz and Olden.

The Examiner has rejected Claims 4 and 8 as unpatentable over teachings of Mi, Olden and Aziz and further in view of Thomlinson. In this Office Action, the Thomlinson patent is cited only for its teachings found in Col. 10, lines 11-16. In the cited passage, Thomlinson describes successive steps of decrypting a master key and master authentication key, decrypting an item key and item authentication key, and then decrypting the actual data item. There is nothing in the cited passage which teaches or suggests using a second key, encrypted using a first key, in an algorithm that generates a session key which is used to decrypt the data. No mention is made of session keys in the Thomlinson passage. Applicants respectfully assert, therefore, that the addition of the Thomlinson patent teachings does not obviate the invention as set forth in Claims 4 and 8.

With regard to the rejection of Claims 9-10, 14 and 17 as unpatentable over Mi in view of Aziz and Olden and further in view of Jablon, Applicants respectfully rely on the arguments set forth above with regard to the teachings

Y0999-558

-17-

Serial No. 09/468,377

Art Unit No. 2134

of the Mi patent, alone and in combination with Aziz and Olden. The Mi patent simply does not teach that a key is known only to the client ("a" in Claims 9-11, 14 and 17) or known only to the content provider ("b" in Claims 9-11, 14 and 17). Moreover, the teachings cited from the Jablon patent, from Col. 7, lines 16-27, do not provide those teachings which are missing from Mi, Aziz and Olden. What Jablon teaches is that a user creates "the user's hidden password, which is maintained as a shared secret and stored securely with the host" (see: Col. 7, lines 18-20). Therefore, the password is known to both the user and the host. Clearly Jablon is not providing the teachings which are missing from the Mi, Aziz and Olden patents.

Finally, the Examiner has cited the Applied Cryptography reference for its teachings regarding MAC authentication procedures. Applicants respectfully assert that the reference does not provide the teachings which are missing from the Mi, Aziz, Olden, Thomlinson and Jablon patents. Moreover, Applicants contend that the Examiner has failed to show how the MAC authentication procedures would be integrated into the teachings of the combined references. The Examiner concludes that "[b]oth client and server

YO999-558

-18-

Serial No. 09/468,377
Art Unit No. 2134

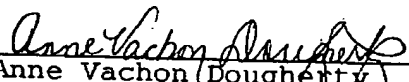
generate the same key during the authentication procedure so the MAC authentication would be an easy way to check authenticity without needing security". Applicants disagree with the Examiner's conclusion and again contend that a *prima facie* case of obviousness has not been established.

Based on the foregoing remarks, Applicants respectfully request reconsideration of the claim language in light of the remarks, withdrawal of the rejections, and allowance of the claims.

Respectfully submitted,

Y. Baransky, et al

By:


Anne Vachon (Dougherty)
Registration No. 30,374
Tel. (914) 962-5910

YO999-558

-19-